Schutz der Privatsphäre trotz globaler Überwachung?

Prof. Dr. Hannes Federrath
Sicherheit in verteilten Systemen (SVS)
http://svs.informatik.uni-hamburg.de

Schutz der Privatsphäre trotz globaler Überwachung?

- Privatsphäre = Recht auf informationelle Selbstbestimmung
  - Recht des einzelnen Menschen, grundsätzlich selbst darüber bestimmen zu dürfen, wer wann was über sie oder ihn erfährt

- Globale Überwachung
  - Beobachtung, Datenerhebung und Auswertung von digitalen Spuren, die Menschen und Unternehmen in technischen Systemen bei deren Nutzung hinterlassen

Recht auf informationelle Selbstbestimmung

»Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den *Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten* voraus. …

Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.

Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.«

aus dem Volkszählungsurteil des Bundesverfassungsgerichts
vom 15. Dezember 1983 1 BvR 209/83 Abschnitt C II.1, S. 43

Aufgabe des Staates: Schutz seiner Bürger

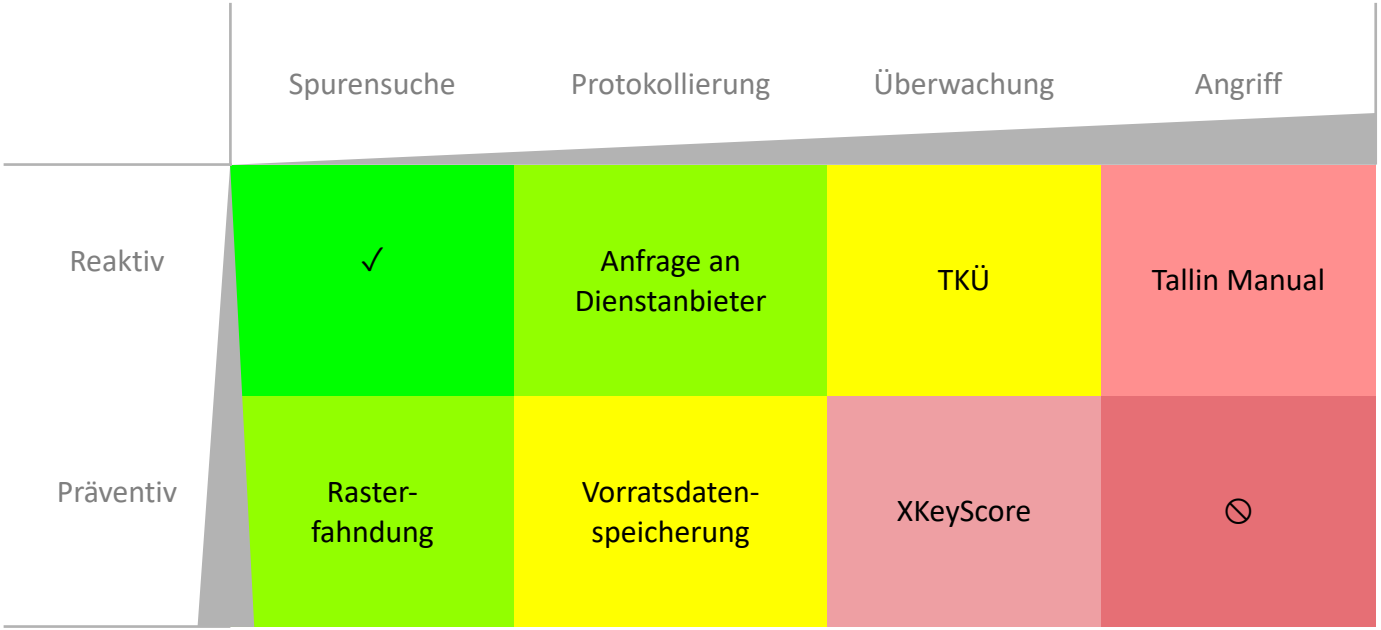
- Thomas Hobbes (1588-1679): Staat als Beschützer der Bürger
  - Der Staat hat das Leben seiner Bürger zu schützen, ebenso dessen Besitz und Freiheit.
  - Staat gibt Regeln für das Zusammenleben der Menschen vor.
  - Je stärker der Staat, umso besser kann er Eigentum und Freiheit schützen.
  - Die Bürger haben dem Staat das Monopol der legitimen Machtausübung gegeben.

nach: Hobbes: Leviathan (1651)

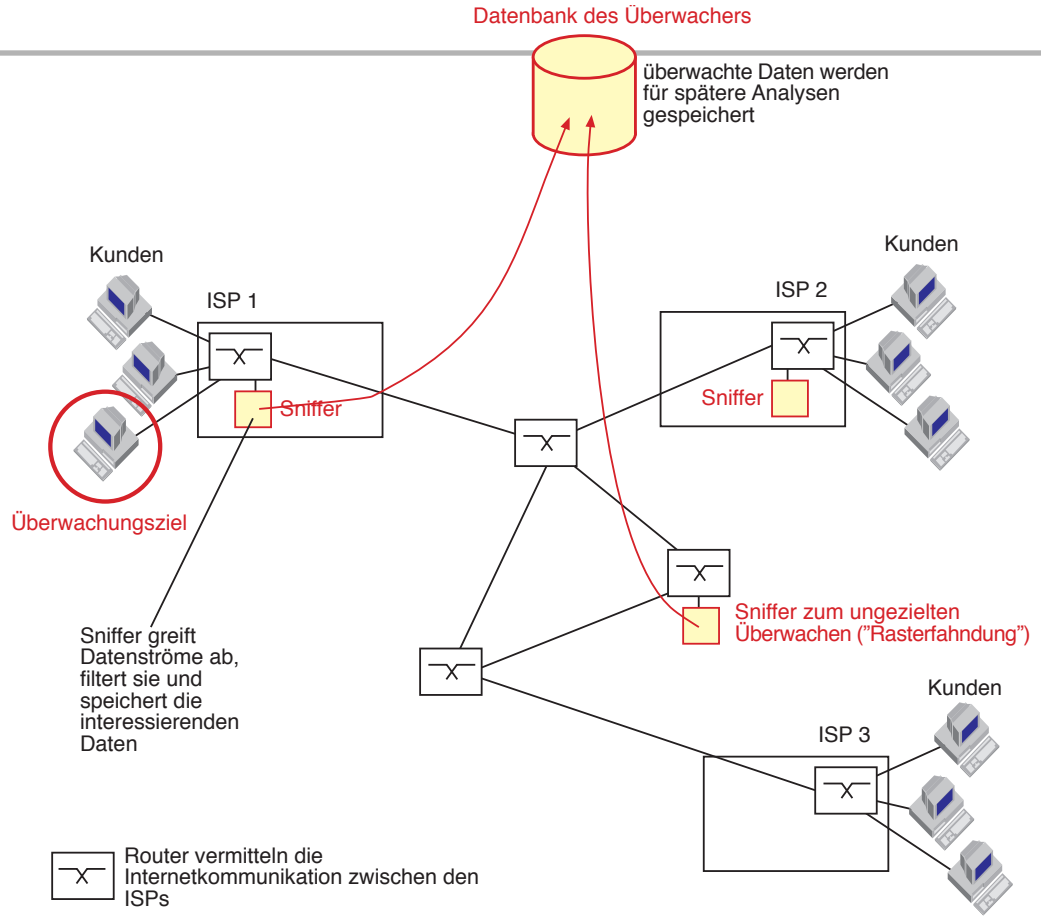
- Problem:
  - Hobbes‘ Staatsmodell ist auch »kompatibel« mit dem Konzept eines Überwachungsstaates.
    - Recht auf informationelle Selbstbestimmung aufgegeben
  - Auch vom Staat gehen Gefahren aus:
    - Am Ende dient der Staat nur noch seiner Selbsterhaltung.

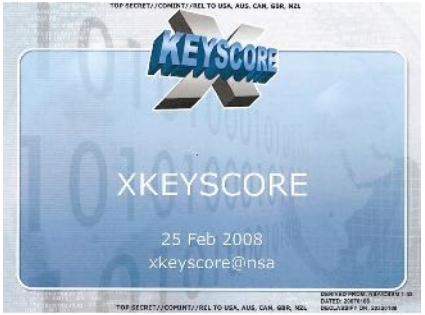
Eingriffstiefe in die Freiheit

- Darf sich der Staat solcher Angriffsmethoden bedienen?

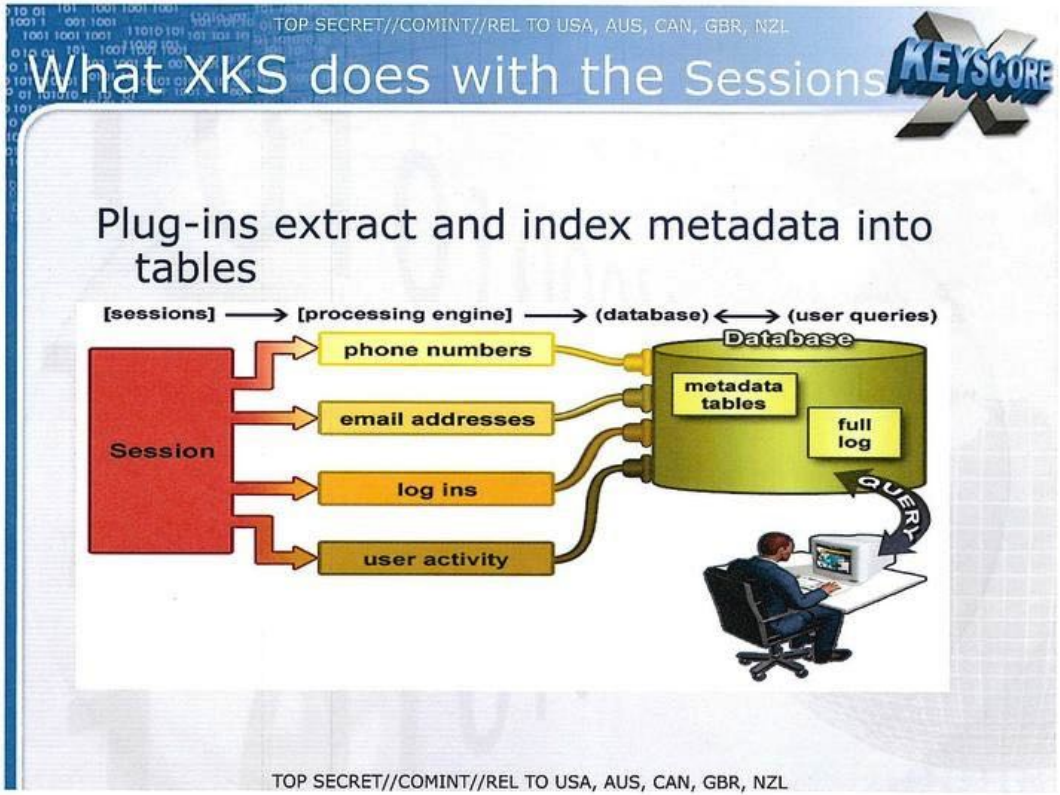


Carnivore


Datenbank des Überwachers
überwachte Daten werden für spätere Analysen gespeichert
Kunden
ISP 1
Sniffer
Überwachungsziel
Sniffer greift Datenströme ab, filtert sie und speichert die interessierenden Daten
Kunden
ISP 2
Sniffer
Sniffer zum ungezielten Überwachen ("Rasterfahndung")
Kunden
ISP 3
Router vermitteln die Internetkommunikation zwischen den ISPs

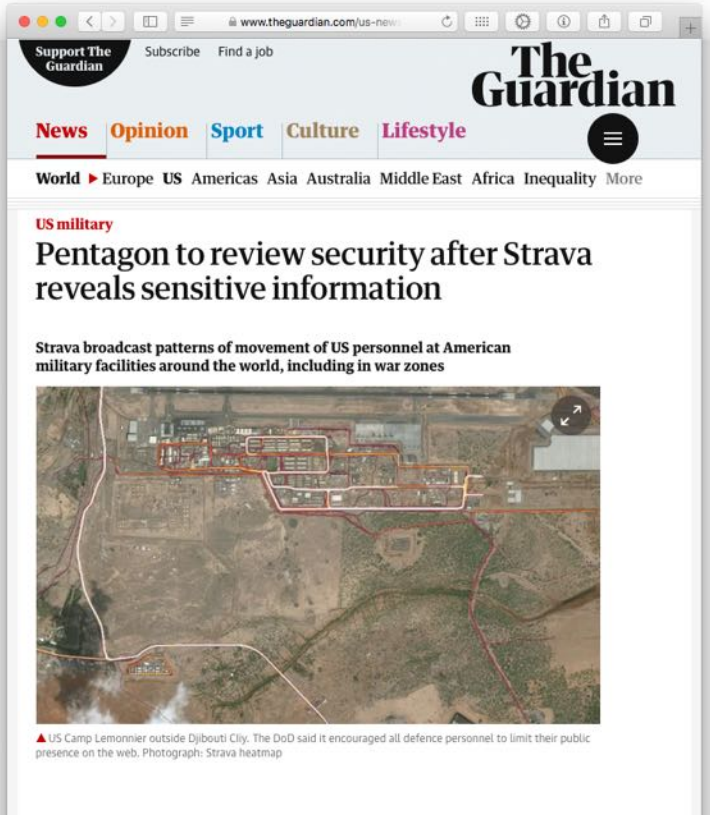


Quelle: Wikimedia



Soziale Netze und Datenschutz – Der Fall »Strava Heatmap«

- Fitness-Tracker Website veröffentlicht beliebte Laufstrecken
- Soldaten des US-Militärs offiziell ausgestattet mit Fitness-Tracker
- Öffentliche »Heatmap« enthüllt ungewollt geheime US-Bases im Ausland



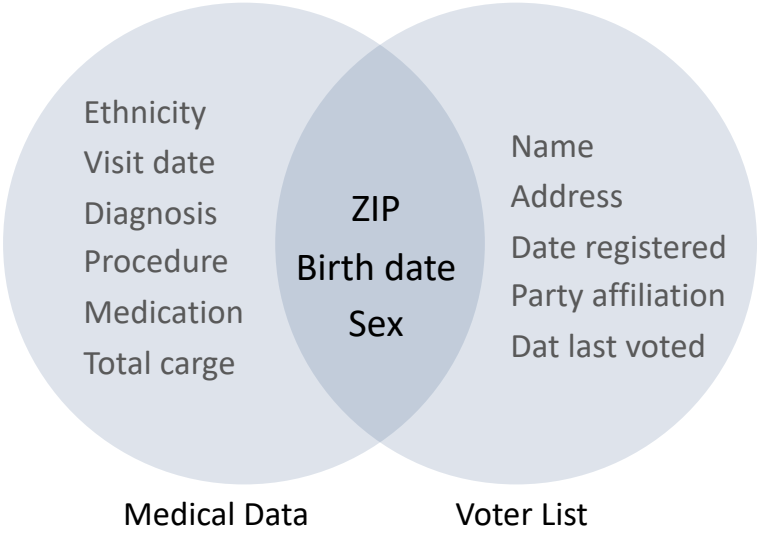
Sources:
https://twitter.com/Nrg8000/status/957318498102865920
https://www.theguardian.com/us-news/2018/jan/29/pentagon-strava-fitness-security-us-military

Verknüpfung von Datensätzen gefährdet Anonymität

Latanya Sweeney, 2000

Vermeintlich anonymes medizinisches Register mit Daten von US-Bürgern…

…wurde verknüpft mit öffentlich zugänglichen US-Wählerverzeichnissen



Beide Datensätze enthalten Geschlecht, Geburtsdatum, Postleitzahl.

Ergebnisse:

- Identifizierung der Krankenakte des ehem. Gouverneurs von Massachusetts, William Weld, war möglich
- Insgesamt 87 Prozent der US-Bevölkerung kann re-identifiziert werden

Latanya Sweeney entwickelte das Konzept der k-Anonymität.

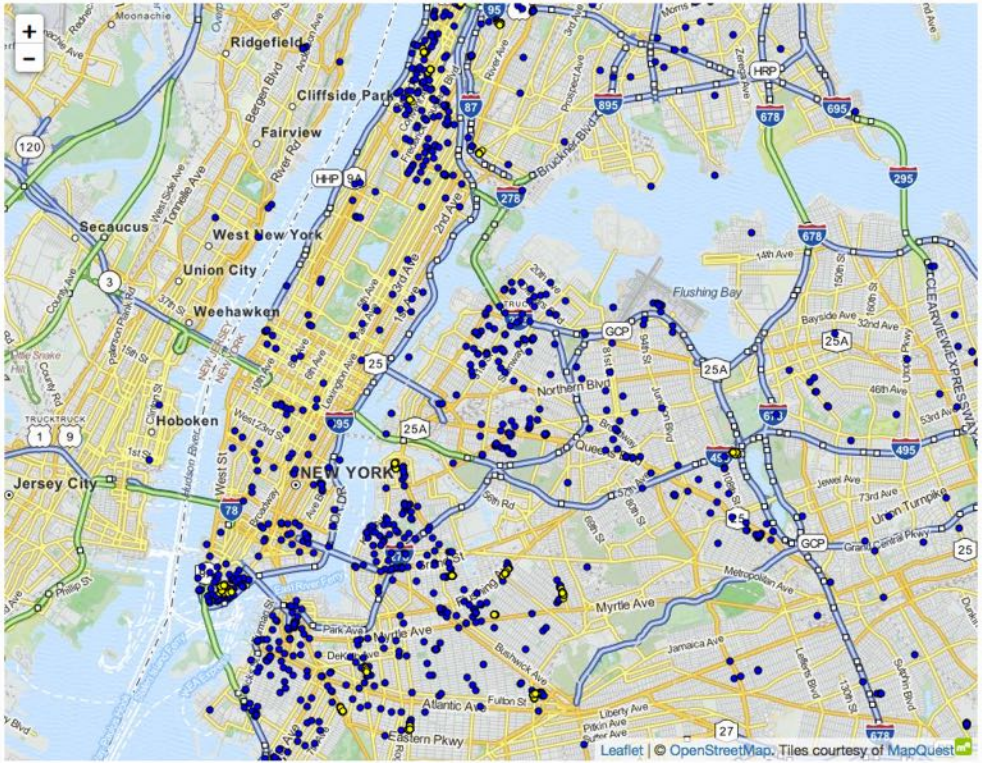
Pseudonymisierte Daten…

…können Persönlichkeitsrechte verletzen.

20 GByte of pseudonymisierter Daten von 170 Mio. Taxifahrten der New Yorker Taxi-gesellschaft

Daten öffentlich abrufbar unter:

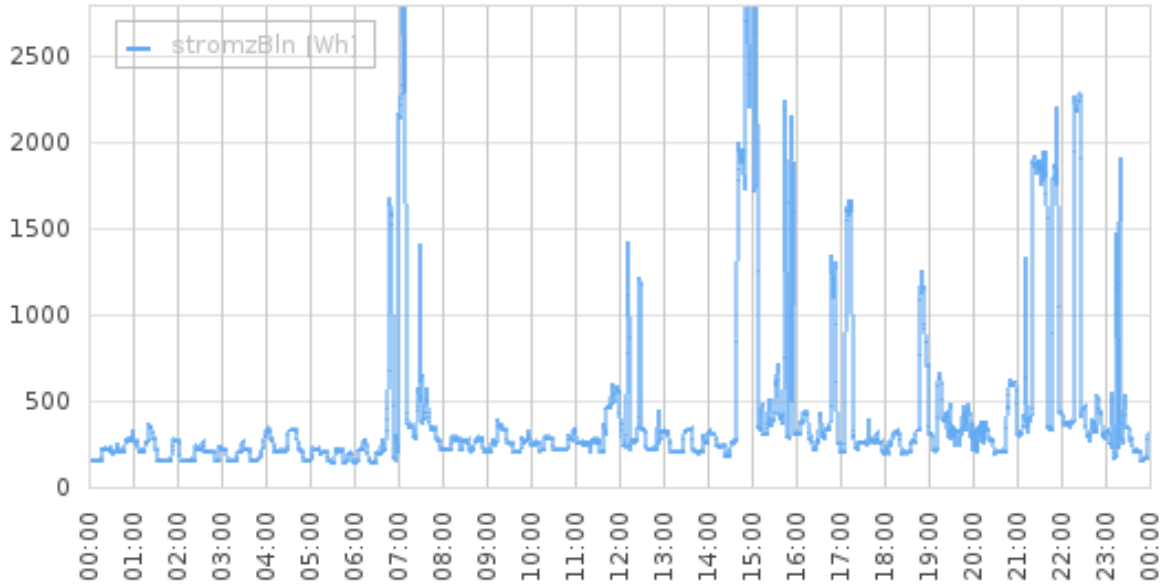
http://www.andresmh.com/nyctaxitrips/



Drop-off locations for trips starting at Larry Flynt's Hustler Club between midnight and 6 am during 2013.

Source: http://content.research.neustar.biz/blog/differential-privacy/stripRaw.html

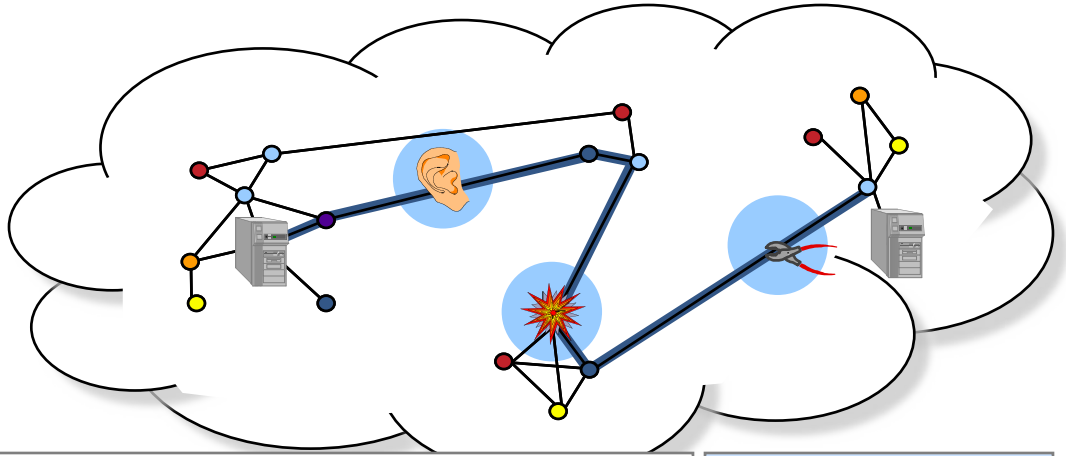
Stromverbrauch verrät Infos über persönliche Lebensverhältnisse



Heutige Rechnernetze

Voydock, Kent, 1983

- verteiltes System



- sehr viele Betreiber
- sehr viele Anwender
- gegensätzliche Sicherheitsinteressen

Bedrohungen:

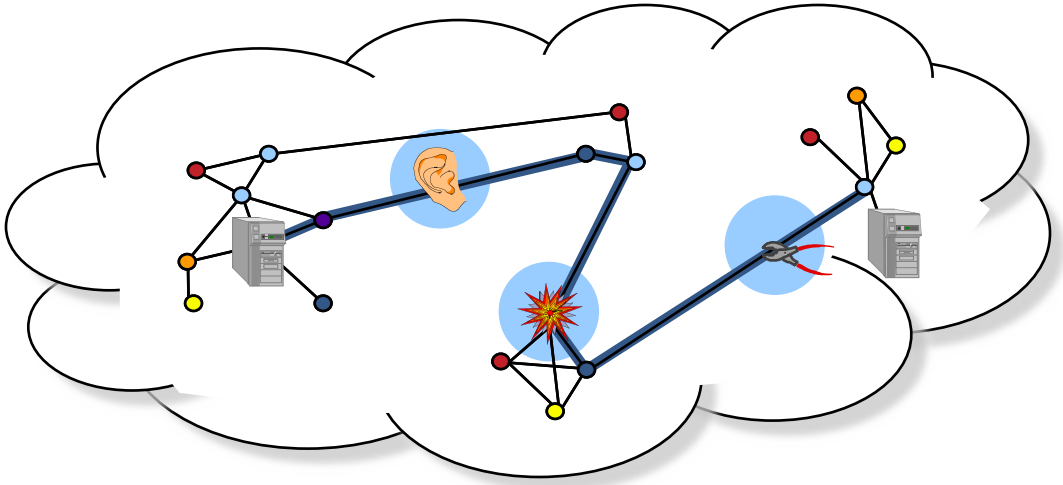
- unbefugter Informationsgewinn
- unbefugte Modifikation
- unbefugte Beeinträchtigung der Funktionalität

Schutz der

- Vertraulichkeit
- Integrität
- Verfügbarkeit

1969 wurde das Internet gegründet.

- verteiltes System

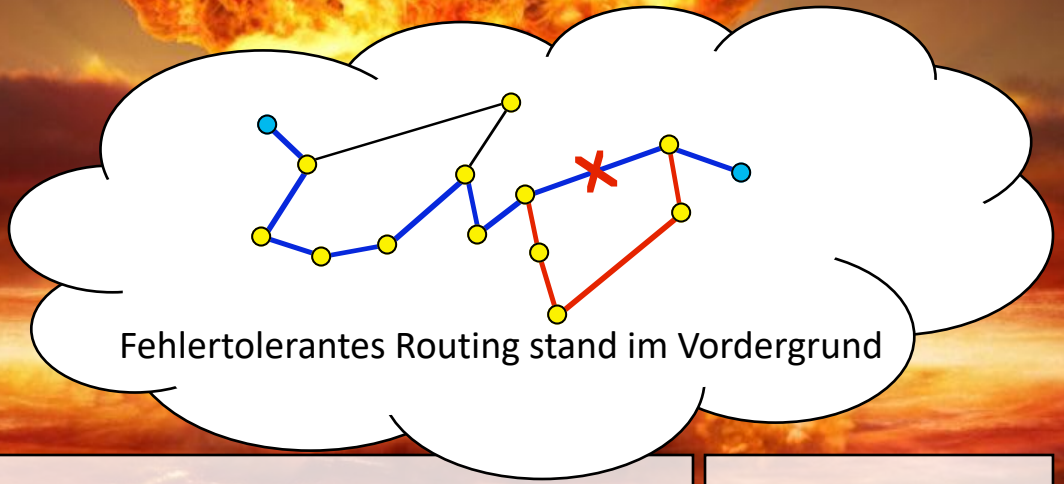


- sehr wenige Betreiber
- wenige Anwender
- kooperativer Ansatz
- geschlossenes System
- Vertrauensmodell

→ unbefugter Informationsgewinn (Vertraulichkeit) und unbefugte Modifikation (Integrität) hatten noch untergeordnete Bedeutung

- Schutz vor außen stehenden Angreifern

	Integrität
unbefugte Beeinträchtigung der Funktionalität	Verfügbarkeit



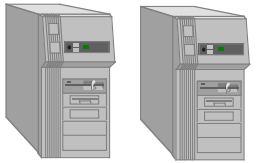
Fehlertolerantes Routing stand im Vordergrund

Bedrohungen:	Schutz der
unbefugter Informationsgewinn	Vertraulichkeit
unbefugte Modifikation	Integrität
unbefugte Beeinträchtigung der Funktionalität	Verfügbarkeit

Foto: Romolo Tavani

Verfügbarkeit: Redundanz und Diversität

- Redundanz
  - Mehrfache Auslegung von Systemkomponenten
  - Bei Ausfall übernimmt Ersatzkomponente
- Diversität
  - Verschiedenartigkeit der Herkünfte
  - Tolerieren von systematischen Fehlern und verdeckten trojanischen Pferden
  - Unabhängige Entwicklung von redundanten (Software)-Komponenten



Beispiel: Doppelung

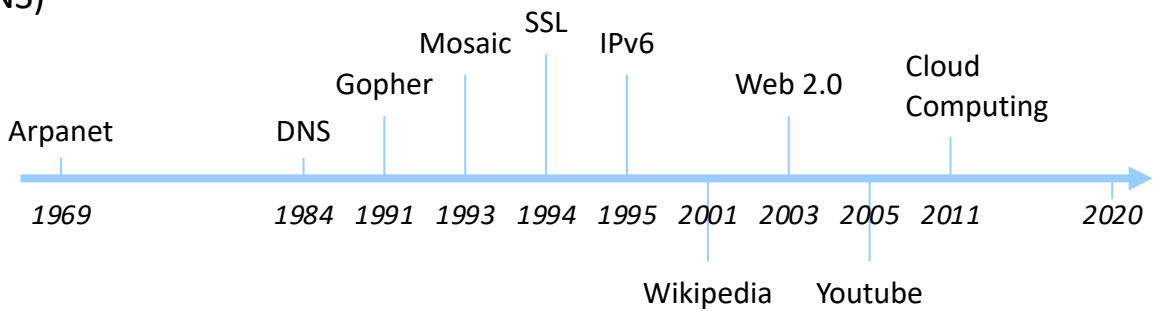
Bedrohungen:	Schutz der
unbefugter Informationsgewinn	Vertraulichkeit
unbefugte Modifikation	Integrität
unbefugte Beeinträchtigung der Funktionalität	Verfügbarkeit

Schutz der Vertraulichkeit und Integrität

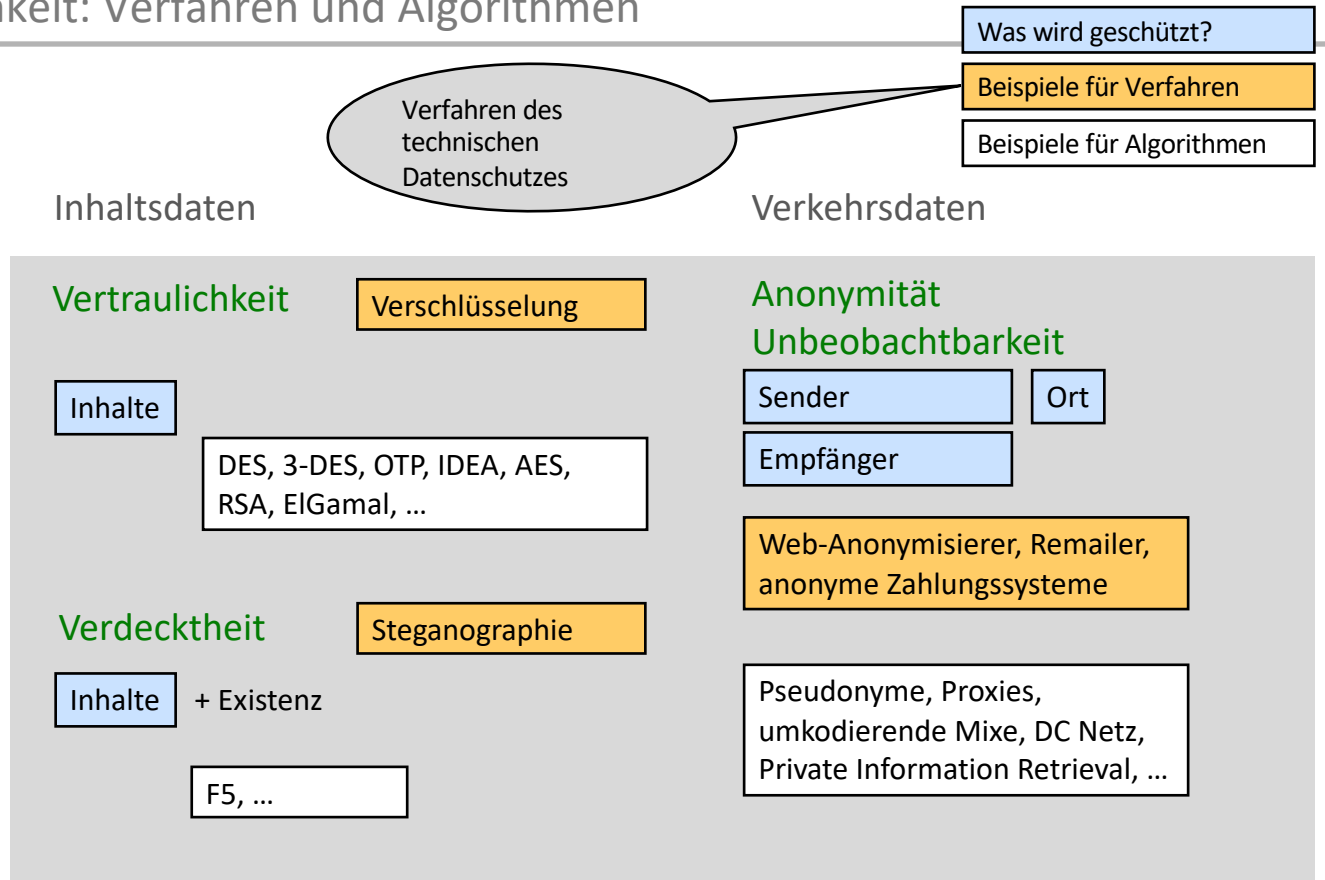
- Erstes tragfähiges Konzept zum Schutz der Vertraulichkeit und Integrität
  - 1994 Secure Sockets Layer (SSL)
  - heute Transport Layer Security (TLS)

SSL/TLS ist auch heute noch die eierlegende Wollmilchsau der IT-Sicherheit im Internet.

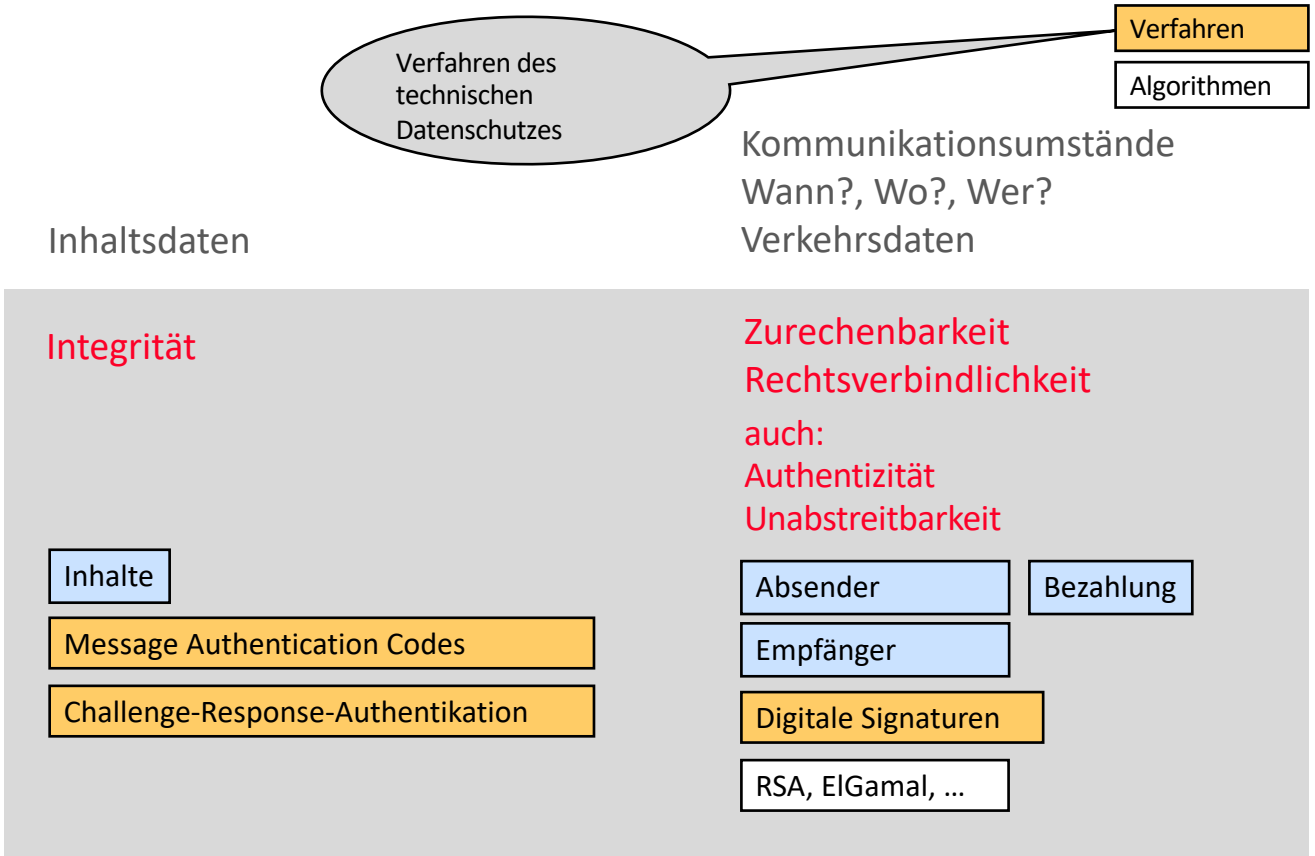
- Zum Vergleich
  - 1969 Arpanet
  - 1984 Domain Name System (DNS)
  - 1991 Hypertext (Gopher)
  - 1993 Webbrowser (Mosaic)



Vertraulichkeit: Verfahren und Algorithmen



Integrität und Zurechenbarkeit, Rechtsverbindlichkeit



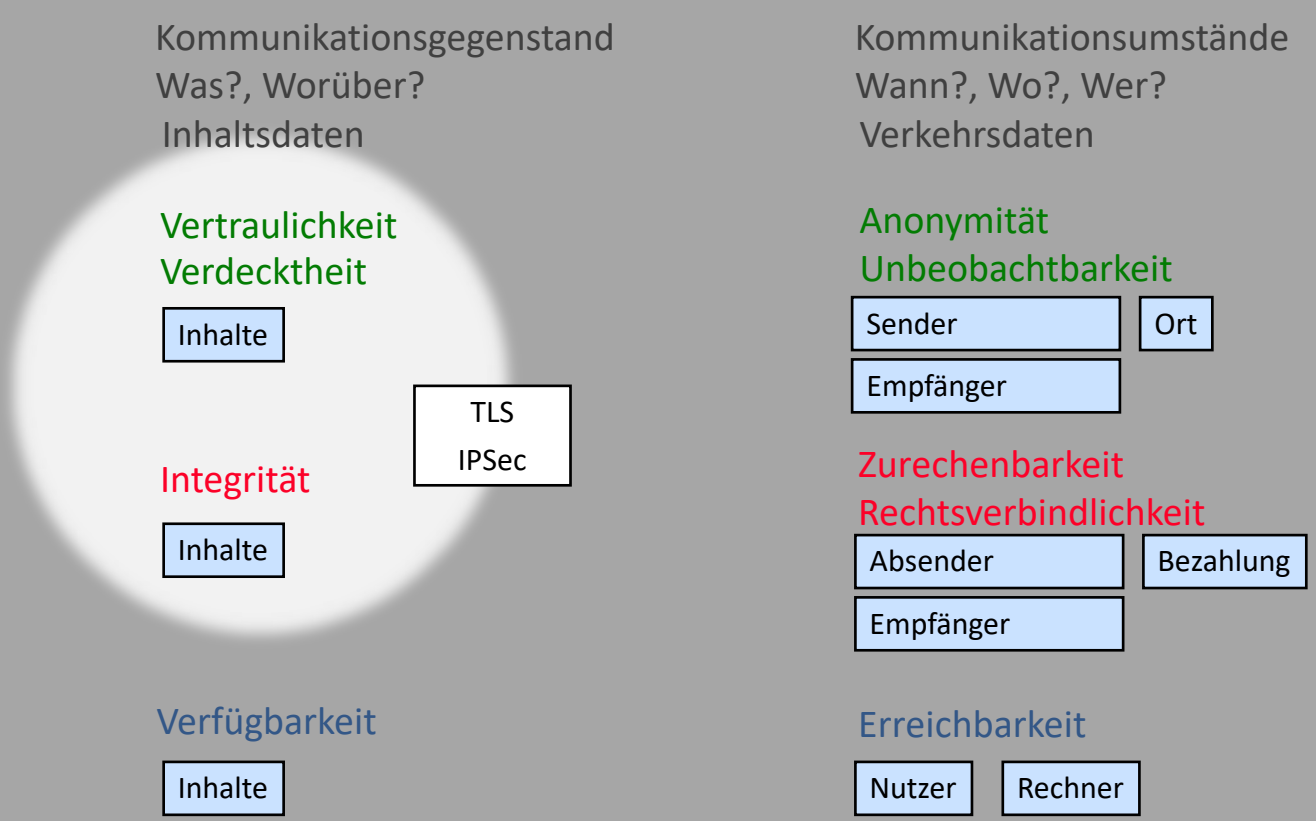
Vertraulichkeit, Integrität und Verfügbarkeit in zwei Dimensionen

Kommunikationsgegenstand Was?, Worüber? Inhaltsdaten	Kommunikationsumstände Wann?, Wo?, Wer? Verkehrsdaten
Vertraulichkeit Verdecktheit Inhalte	Anonymität Unbeobachtbarkeit Sender, Ort, Empfänger
Integrität Inhalte	Zurechenbarkeit Rechtsverbindlichkeit Absender, Bezahlung, Empfänger
Verfügbarkeit Inhalte	Erreichbarkeit Nutzer, Rechner

Vertraulichkeit, Integrität und Verfügbarkeit in zwei Dimensionen

Kommunikationsgegenstand Was?, Worüber? Inhaltsdaten	Kommunikationsumstände Wann?, Wo?, Wer? Verkehrsdaten
Vertraulichkeit Verdecktheit Inhalte	Anonymität Unbeobachtbarkeit Sender, Ort, Empfänger
Integrität Inhalte	Zurechenbarkeit Rechtsverbindlichkeit Absender, Bezahlung, Empfänger
Verfügbarkeit Inhalte, Inet69, IoT, Ubiquitous Computing	Erreichbarkeit Nutzer, Rechner

Vertraulichkeit, Integrität und Verfügbarkeit in zwei Dimensionen



Vertraulichkeit, Integrität und Verfügbarkeit in zwei Dimensionen

Kommunikationsgegenstand
Was?, Worüber?
Inhaltsdaten

Kommunikationsumstände
Wann?, Wo?, Wer?
Verkehrsdaten

Vertraulichkeit
Verdecktheit

Inhalte

Anonymität
Unbeobachtbarkeit

Sender | Ort

Empfänger

Kennzeichnungspflicht für alle Datenpakete

Integrität

Inhalte

Zurechenbarkeit
Rechtsverbindlichkeit

Absender | Bezahlung

Empfänger

Verfügbarkeit

Inhalte

Erreichbarkeit

Nutzer | Rechner

Vertraulichkeit, Integrität und Verfügbarkeit in zwei Dimensionen

Kommunikationsgegenstand
Was?, Worüber?
Inhaltsdaten

Kommunikationsumstände
Wann?, Wo?, Wer?
Verkehrsdaten

Vertraulichkeit
Verdecktheit

Inhalte

Anonymität
Unbeobachtbarkeit

Privacy by Design

Sender

Ort

Empfänger

Integrität

Inhalte

Zurechenbarkeit
Rechtsverbindlichkeit

Absender

Bezahlung

Empfänger

Verfügbarkeit

Inhalte

Erreichbarkeit

Nutzer

Rechner

Vertraulichkeit, Integrität und Verfügbarkeit in zwei Dimensionen

Kommunikationsgegenstand
Was?, Worüber?
Inhaltsdaten

Kommunikationsumstände
Wann?, Wo?, Wer?
Verkehrsdaten

Vertraulichkeit
Verdecktheit

Inhalte

Anonymität
Unbeobachtbarkeit

Sender | Ort

Empfänger

Privacy by Design

stehen meist im Widerspruch zueinander

Kennzeichnungspflicht für alle Datenpakete

Integrität

Inhalte

Zurechenbarkeit
Rechtsverbindlichkeit

Absender | Bezahlung

Empfänger

Verfügbarkeit

Inhalte

Erreichbarkeit

Nutzer | Rechner

Die 7 Grundprinzipien der Privacy by Design

https://www.privacybydesign.ca

1. Proaktiv, nicht reaktiv – als Vorbeugung und nicht als Abhilfe
2. Datenschutz als Standardeinstellung
3. Datenschutz ist in das Design eingebettet
4. Volle Funktionalität – eine Positivsumme, keine Nullsumme
5. Durchgängige Sicherheit – Schutz während des gesamten Lebenszyklus
6. Sichtbarkeit und Transparenz – für Offenheit sorgen
7. Die Wahrung der Privatsphäre der Nutzer – für eine nutzerzentrierte Gestaltung sorgen

Entwickelt von Ann Cavoukian beim Information & Privacy Commissioner Ontario, Canada in den 1990er Jahren

Privacy by Design

- Stand der Technik
- Kosten
- Art, Umfang, Umstände, Zwecke
- Privacy by Default (PbD)
- Risiko-management
- Technisch-organisatorische Maßnahmen

Art, Umfang, Umstände, Zwecke

- Verbot mit Erlaubnisvorbehalt
  - Einwilligung
  - Erforderlichkeit
  - Direkterhebung

Privacy by Default (PbD)

- Beschränkung auf Verarbeitungszweck
- Beschränkung des Umfangs
- Beschränkung auf Speicherfristen
- Beschränkung der Zugänglichkeit

Technisch-organisatorische Maßnahmen

- Datenschutz-grundsätze
- Betroffenen-rechte

Datenschutz-grundsätze

- Transparenz (PbD)
- Zweckbindung
- Daten-sparsamkeit
  - Anonymität
  - Unbeobachtbarkeit
- Datensicherheit (PbD)
  - Pseudonymisierung
  - Verschlüsselung
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - Belastbarkeit
  - Wiederherstellbarkeit
  - Notfallmanagement
  - Überprüfbarkeit
  - Bewertung
  - Evaluierung

Betroffenen-rechte

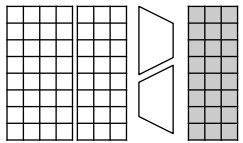
- Transparenz
- Benachrichtigung
- Auskunft
- Berichtigung
- Löschung
- Widerspruchsrecht
- Recht auf Vergessenwerden
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit

PbD

Privacy by Design (PbD): Schnittmenge von PbD nach der DSGVO und PbD nach Cavoukian

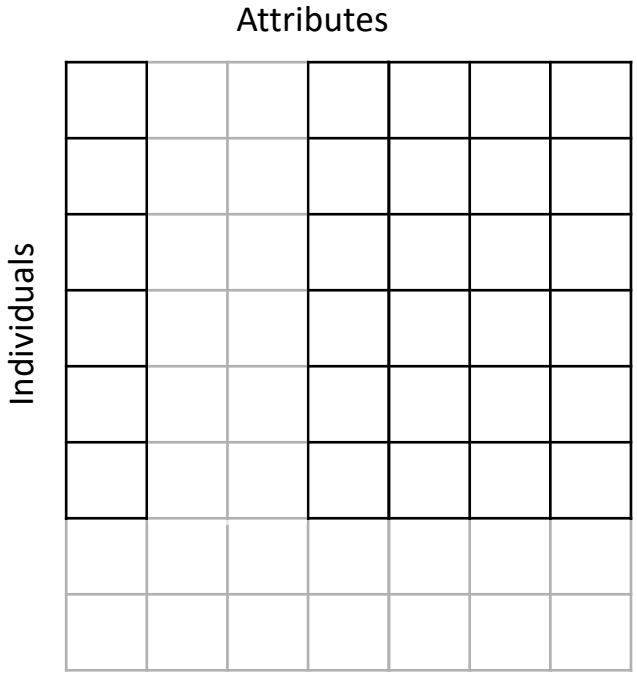
Privacy by Design

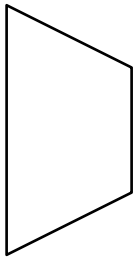
- Stand der Technik
- Kosten
- Art, Umfang, Umstände, Zwecke
  - Verbot mit Erlaubnisvorbehalt
    - Einwilligung
    - Erforderlichkeit
    - Direkterhebung
- Privacy by Default
  - Beschränkung auf Verarbeitungszweck
  - Beschränkung des Umfangs
  - Beschränkung auf Speicherfristen
  - Beschränkung der Zugänglichkeit
- Risiko-management
- Technisch-organisatorische Maßnahmen
  - Datenschutz-grundsätze
    - Transparenz
      - Enforce
      - Inform
      - Control
      - Demonstrate
    - Zweckbindung
    - Daten-sparsamkeit
      - Anonymität
      - Unbeobachtbarkeit
      - Minimise
      - Separate
      - Aggregate
      - Perturbate
      - Hide
    - Datensicherheit
      - Pseudonymisierung
      - Verschlüsselung
      - Vertraulichkeit
      - Integrität
      - Verfügbarkeit
      - Belastbarkeit
      - Wiederherstellbarkeit
      - Notfallmanagement
      - Überprüfbarkeit
      - Bewertung
      - Evaluierung
  - Betroffenen-rechte
    - Transparenz
    - Benachrichtigung
    - Auskunft
    - Berichtigung
    - Löschung
    - Widerspruchsrecht
    - Recht auf Vergessenwerden
    - Recht auf Einschränkung der Verarbeitung
    - Recht auf Datenübertragbarkeit



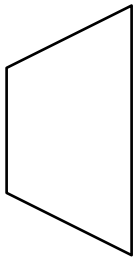
Privacy design strategies

in Anlehnung an Hoepman, 2014

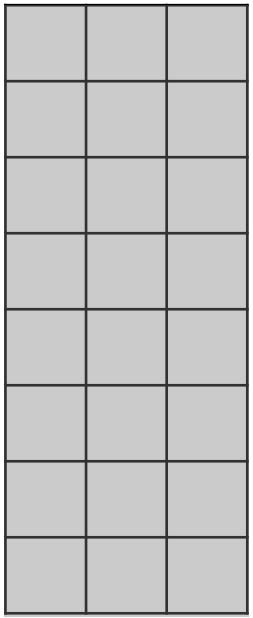




aggregate



perturbate

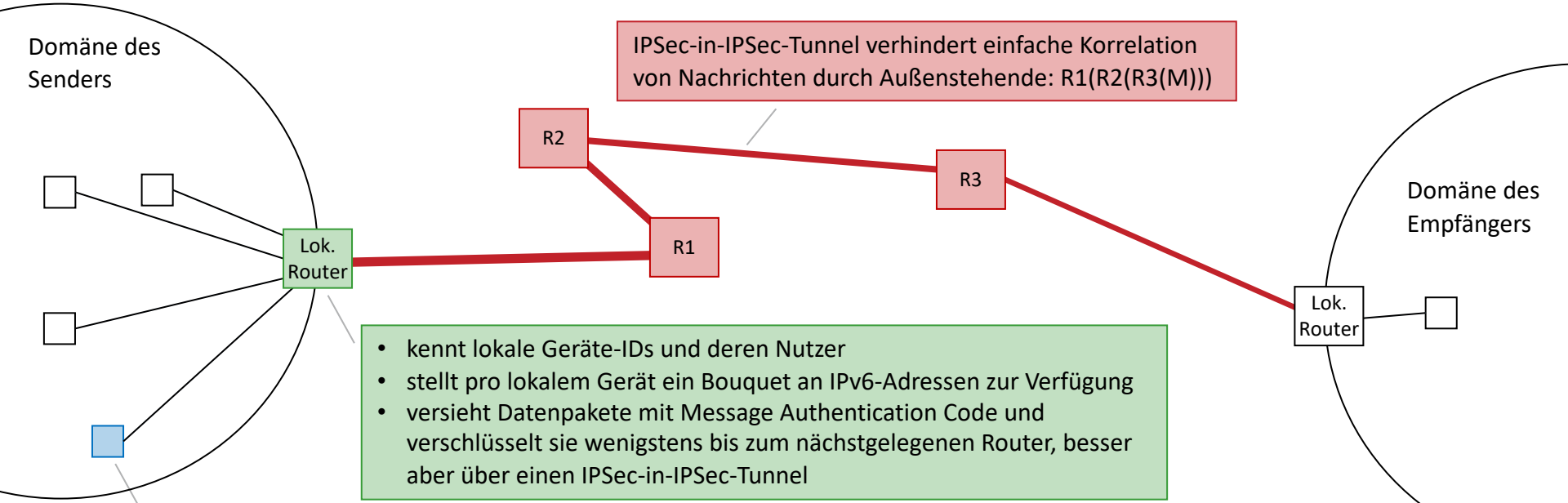


minimise

separate

hide

Kombination sinnvoller und (halbwegs) skalierbarer Techniken



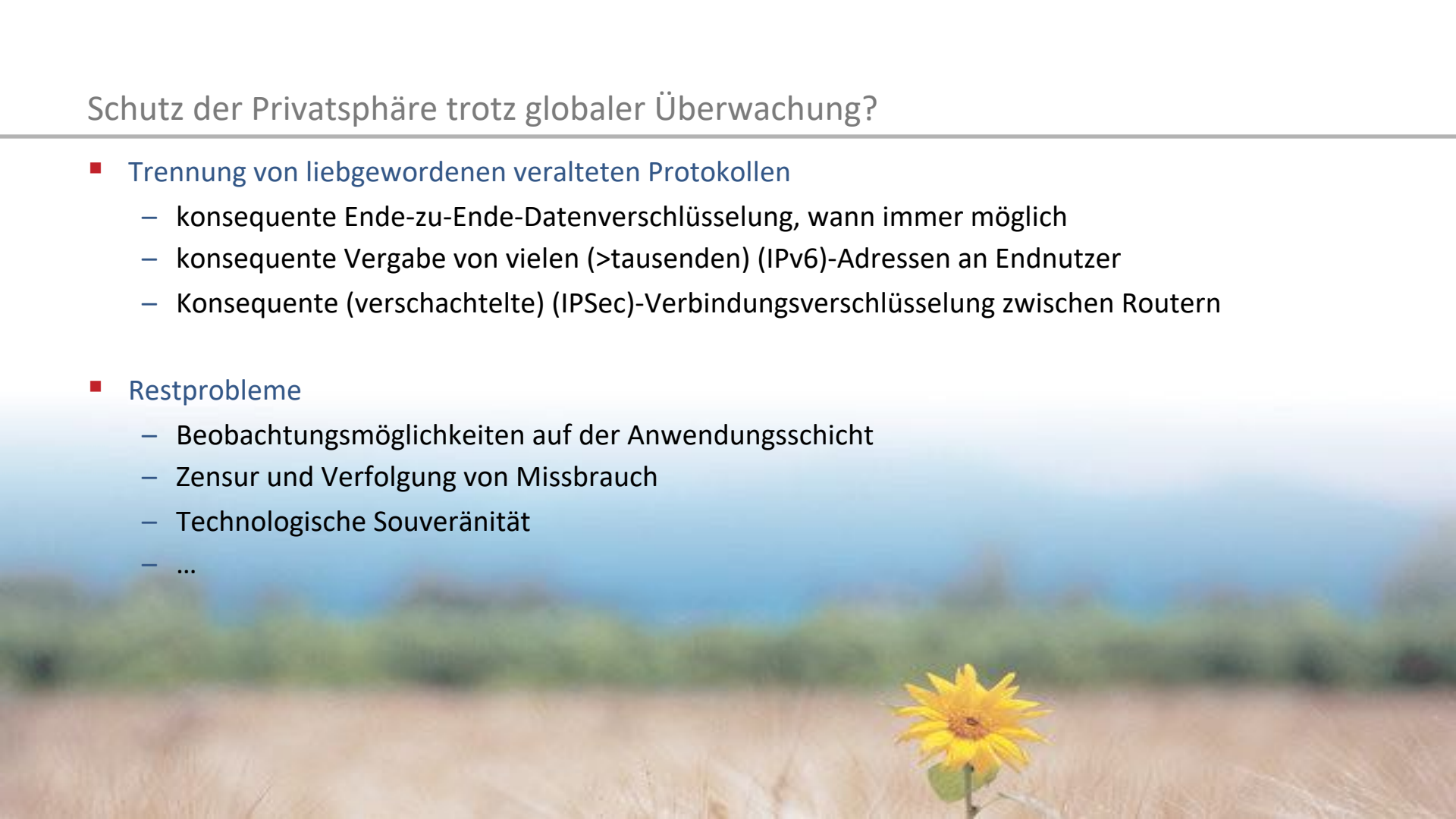
Privacy by Design

- Stand der Technik
- Kosten
  - ROSI
- Art, Umfang, Umstände, Zwecke
- Privacy by Default
  - Verbot mit Erlaubnisvorbehalt
    - Einwilligung
    - Erforderlichkeit
    - Direkterhebung
  - Beschränkung auf Verarbeitungszweck
    - Beschränkung des Umfangs
    - Beschränkung auf Speicherfristen
    - Beschränkung der Zugänglichkeit
- Risiko-management
- Technisch-organisatorische Maßnahmen
  - Datenschutz-grundsätze
    - Transparenz
      - Policy
      - Big Data
      - Bereitschaft und gute Dokumentation
      - Algorithmen
        - Enforce
        - Inform
        - Control
        - Demonstrate
    - Zweckbindung
    - Daten-sparsamkeit
      - Anonymität
      - Unbeobachtbarkeit
      - Minimise
      - Separate
      - Aggregate
      - Perturbate
      - Hide
    - Datensicherheit
      - Pseudonymisierung
      - Verschlüsselung
      - Vertraulichkeit
      - Integrität
      - Verfügbarkeit
      - Belastbarkeit
      - Wiederherstellbarkeit
      - Notfallmanagement
      - Überprüfbarkeit
      - Bewertung
      - Evaluierung
  - Betroffenen-rechte
    - Transparenz
    - Benachrichtigung
    - Auskunft
    - Berichtigung
    - Löschung
    - Widerspruchsrecht
    - Recht auf Vergessenwerden
    - Recht auf Einschränkung der Verarbeitung
    - Recht auf Datenübertragbarkeit
    - Bereitschaft

Schutz der Privatsphäre trotz globaler Überwachung?

- Trennung von liebgewordenen veralteten Protokollen
  - konsequente Ende-zu-Ende-Datenverschlüsselung, wann immer möglich
  - konsequente Vergabe von vielen (>tausenden) (IPv6)-Adressen an Endnutzer
  - Konsequente (verschachtelte) (IPSec)-Verbindungsverschlüsselung zwischen Routern

- Restprobleme
  - Beobachtungsmöglichkeiten auf der Anwendungsschicht
  - Zensur und Verfolgung von Missbrauch
  - Technologische Souveränität
  - …



inf.uni-hamburg.de

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

DEPARTMENT OF INFORMATICS
SECURITY AND PRIVACY

HOME COURSES THESES RESEARCH PEOPLE SERVICE

UHH → MIN-Fakultät → Fachbereich Informatik → Einrichtungen → Arbeitsbereiche → Security and Privacy → Home

WORKING GROUP ON «SECURITY AND PRIVACY»

Security and Privacy

Information systems become more and more important in critical infrastructures, while the Internet has evolved to a critical infrastructure itself. The secure operation of these infrastructures is vital and their failure can have severe impacts up to the loss of human lives.
Security refers to the fact that protection goals are achieved in the presence of malicious attacks and system failures. Typical security goals can be confidentiality, integrity, accountability, and availability. Security and privacy in information systems addresses both technical and organizational aspects, such as building and establishing security concepts and security infrastructures as well as risk analysis and risk management.
Privacy can be a conflicting goal to security, but they can also benefit from each other. Hence, it is necessary to balance both when developing secure information systems.

Prof. Dr. Hannes Federrath
Fachbereich Informatik
Universität Hamburg
Vogt-Kölln-Straße 30
D-22527 Hamburg

Telefon +49 40 42883 2358

federrath@informatik.uni-hamburg.de

https://svs.informatik.uni-hamburg.de